Data Immersion

Exercise 5.3

8/23/23

Micky Smith

Data Ethics: Security & Privacy

Step 1:

- **Is this a data privacy issue, data security issue, or both? Please provide a short explanation for your answer.**
  - This would be both a data privacy issue and data security issue.
  - It's a data privacy issue because Pig E. Bank has policies that have been specified to its clients regarding how they will handle and store personal information to ensure their client's privacy.
  - It's a data security issue because the investigator has agreed to uphold the data security policy set it place by Pig E. Bank.
- **What would be the risks to Pig E. Back and its customers if this issue weren't addressed?**
  - The photo is a risk of a security breach and could be used to compromise the client's privacy. If it's not appropriately addressed, Pig E. Bank and the investigator could be subject to financial and legal consequences.
- **To prevent this type of data theft in the future, what changes would need to be made to the policies around data access?**
  - Increased training for employees in handling client information, with stronger repercussions for employees who don't appropriately follow security guidelines. Look into encrypting client's personal data when on screen, as well as providing extensive onscreen warnings when client PII is prevented.

Step 2:

- **Does this scenario highlight a data privacy issue, data security issue, or some other ethical issue?**
  - This would highlight both a data privacy issue and data security issue. This could violate the data security implications set by Pig E. Bank by providing access to data in geographical areas that don't need to comply with the same data privacy laws set in the country Pig E. Bank does business.
- **How would you communicate your concerns to the compliance committee?**
  - I would communicate my concerns by providing an understanding of the importance of meeting the security requirements and privacy standards we have set for our clients. I would acknowledge the benefits of the cost savings, but express that the implications of not meeting security requirements can inevitably cost more. And last, I would provide a resolution towards how we could still remain compliant of our security and privacy guidelines while still potentially look into outsourcing.
- **If Pig E. Bank does go ahead and outsource some of its analytical functions, how would you anonymize the data while ensuring that someone can still conduct an analysis?**

- We would use differential privacy to provide a higher level of anonymization to the data. As well, we could use encryptions and scrubbing customer identifiers that would still allow analysis, this may still leave some data security risks however.

Step 3:

- **Research a case study from your own country where a company or organization has acted unethically in terms of collecting and sharing data. You're free to use information you find on the internet, but make sure you include the link to your resources in your document.**
  - Equifax data breach FAQ: What happened, who was affected, what was the impact? | CSO Online
  - Equifax data breach occurred because of hackers sending an HTTP request with a malicious code exposing a vulnerability in out of data software within Apache Struts. The patch for this vulnerability was provided and distributed to the company on March 9th, but an employee that should have done so didn't. The scans they ran on March 15th did not flag any vulnerable systems still showing.
  - This was a privacy issue since it allowed millions of customer's personal data to be accessed by hackers.
  - This is also a security issue because the employees of the company didn't initiate the update according to the company request.
- **Explain what the company or organization did exactly. Did they act according to regional or national laws?**
  - The company implemented a patch that would take care of the vulnerability within their system. Once the patch wasn't enforced, and customer information was released publicly, they created a separate dedicated domain, Equifaxsecurity2017.com, to host the site with information and resources for those potentially affected.
- **Why was the company's behavior unethical? (To answer this question, you can refer to this exercise and the previous exercise on data bias.)**
  - The unethical behavior was more focused on the act of their employees than the company itself. They attempted to implement a patch to their security that would have kept the vulnerability from furthering. This helped the data breach spread to customer information and caused the privacy issue.
- **What could you and the company have done to prevent this unethical behavior? Please provide some concrete suggestions.**
  - The company could have done more to ensure that the patch didn't fail to be implemented for a basic vulnerability. And had better measures to ensure the patch didn't go neglected.
  - The company had data provided among multiple systems within their system, because of which it was easier for the hackers to obtain customer information. Something I could have done as a data analyst, provide reasoning for placing information under a better encrypted and single system instead of having it within multiple locations.
  - Equifax's system was not encrypted enough to keep their customer's data private. Their system was able to provide customer information to any "trusted" device. Their system could have been better encrypted in order to ensure that only the customer with authorization saw private information.

- I could have provided an outline towards how we could be more aware of strange anomalies occurring that could cause a breach in customer's private information.